www.net-patrol.com

‘Information and Cyber Security’

NPI

Tom Warren

CSX,CRISC,ACE,FRSA,PI

Strategic Security Plan

The main points:

- Improved Awareness
- Proactive risk management
- How to react in a incident or crisis situation.

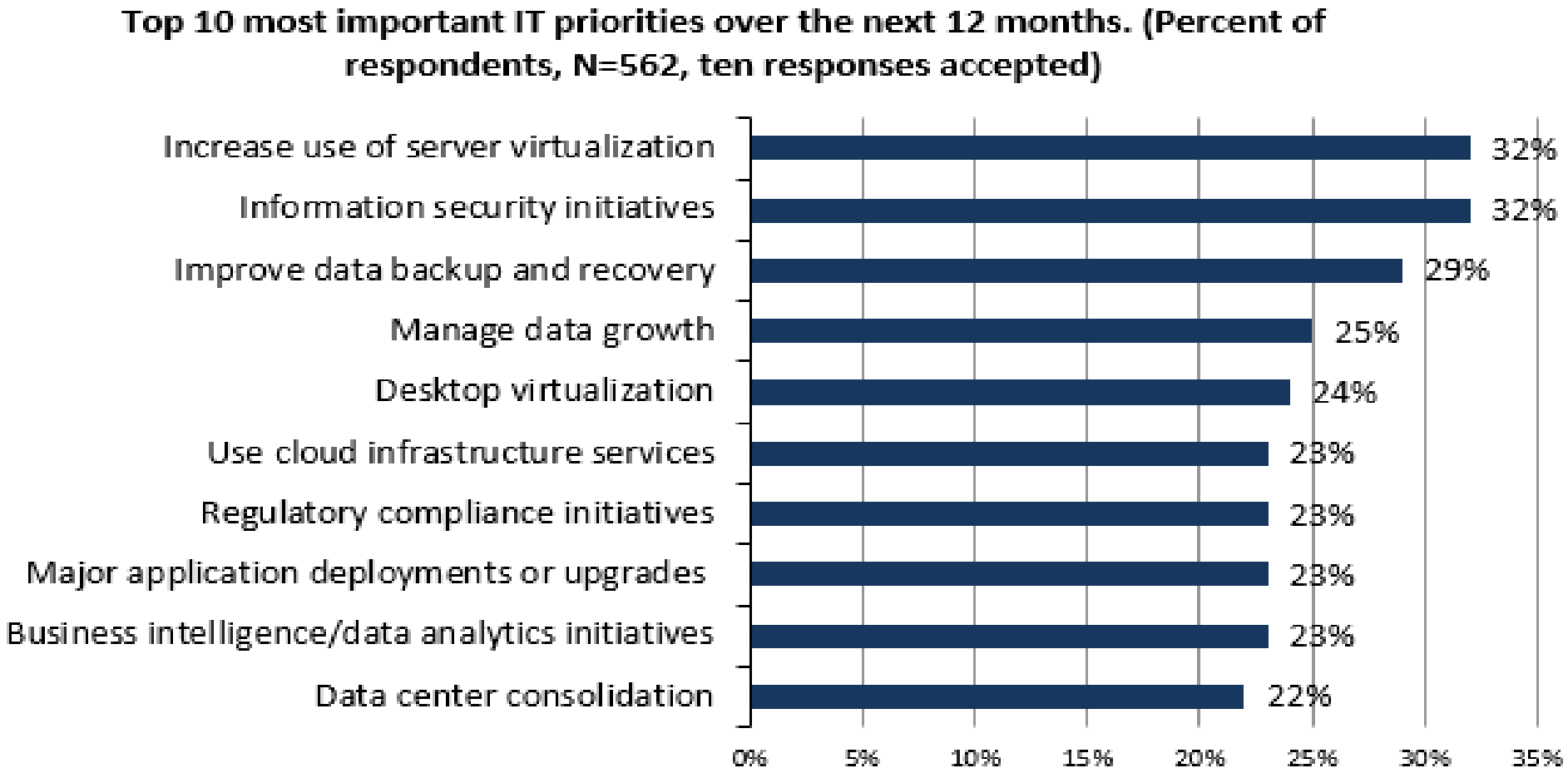
Security is not a destination, it’s a continual improvement on the environment. Most SSPs can be met in 3 years. While aggressive, there could be some great controls already in place. Using what has already been put in place can see real cost savings. ‘Reinventing the wheel’ does not always need to be done.

Haven’t we already done this?

- ERM – ISO 31000/other ISOs
- Information Security – ISO 27001/05
- Understanding the difference
- Importance of Control Frameworks
- Vendor Impact
- Are there others?
- What is the best framework to use?
- How often is this reviewed?

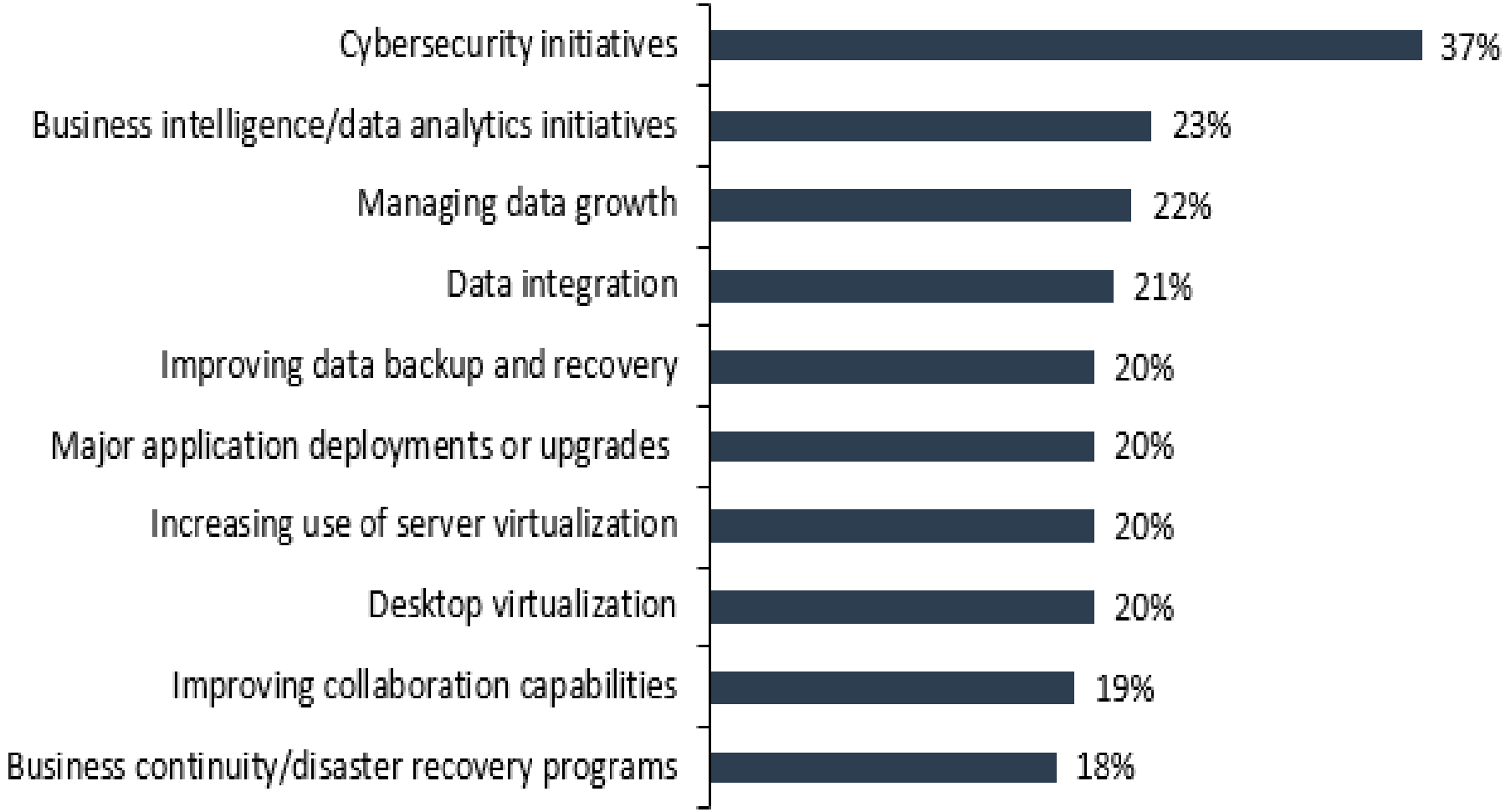
Transit from ISO 27001 Risk Management to ISO 31000 based Risk Management_.pdf

‘Why do Cyber/InfoSec?’



Source: Enterprise Strategy Group, 2014.

Top 10 most important IT priorities over the next 12 months. (Percent of respondents, N=633, ten responses accepted)



Source: Enterprise Strategy Group, 2016.

Why is this needed, why is this so important?

- High risk of information breach, leakage, or lost.
- This would be a crisis situation from a reputation/financial loss standpoint
- The reputation to the public and investors/members is by far, the most essential asset that must be protected.
- Think about what would happen if a breach of the information happened in your own company, or one of your clients.
- What is the plan if this does happen?
- Governance provides the needed controls to help eliminate or stop such risks.

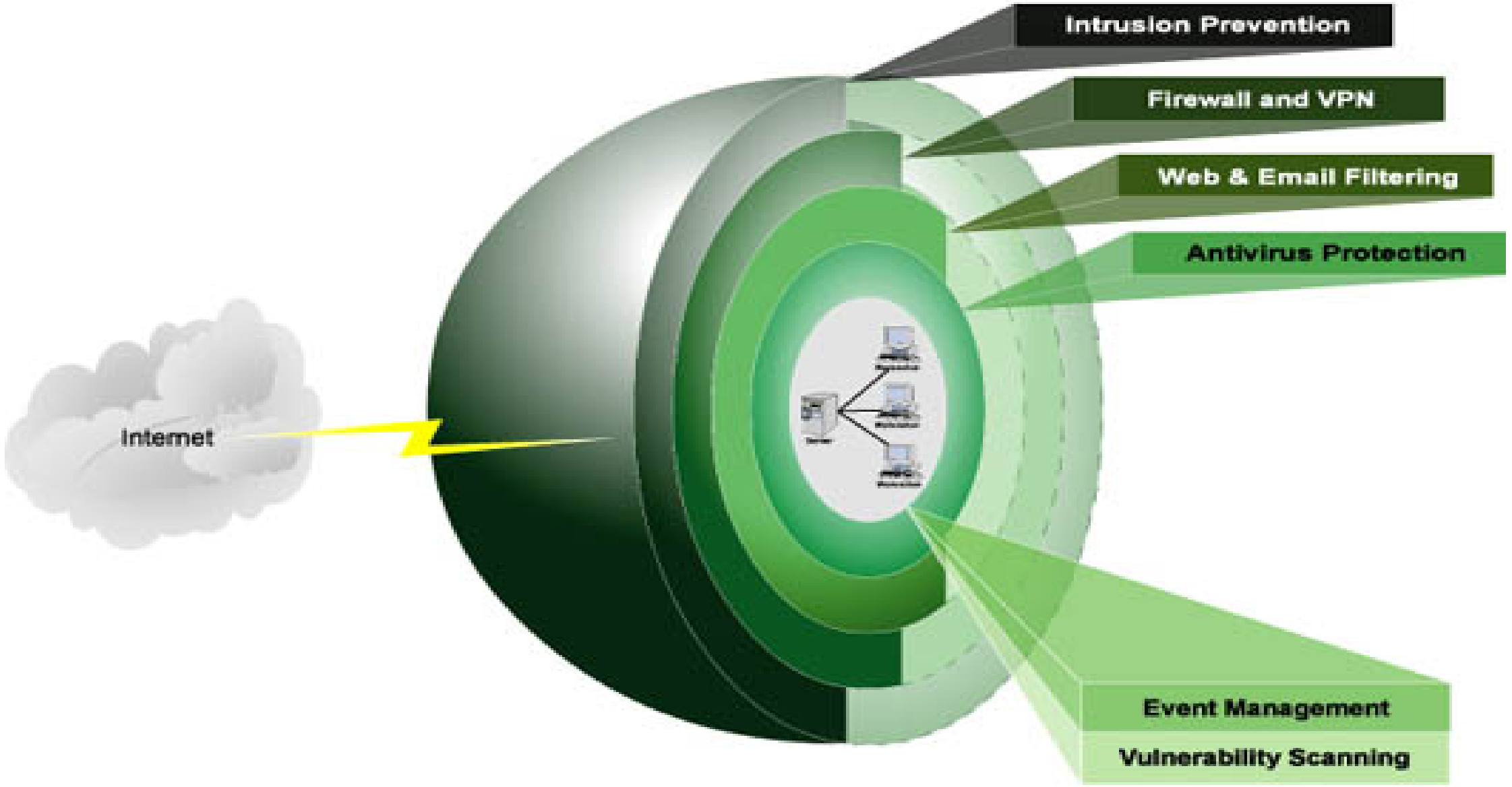
What can happen?

- There are two main threats to an environment
  - Insider threat/Outsider threat
- Insider threat can be via mistake, misuse, or disgruntlement
- The insider threat is more likely to harm a business/organization than an outsider threat.
- Outsider threat is that caused by ‘hacking’ ‘infecting’ or ‘interrupting’
- Groups provide services for such outsider threats.
- Movements exist today as a ‘collective’. Example: Anonymous
- Motives for such are usually revenge or ‘pay-back’.

What is Cyber/ Information Security?

Information security (sometimes shortened to InfoSec) is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...)

‘The Changing Face of IT Security’



‘What was missing in the previous model?’

- Physical security
  - Site survey
- DR/BCP/Cybersecurity aspects
  - Understand which solution will work
- Policy/Governance
  - Hardening guidelines
  - Encryption solutions
  - Penetration testing (secondary to Vulnerability Testing)
  - Minimum Security Requirements
  - Standards/Process Policy

‘Solutions’

- A time of ‘married disciplines’ is here.
- Site surveys, IT assessments, Cyber/InfoSec audits must work together.
- Provides streamline processes, and budget savings through automated alerts.
- Using an Cyber/InfoSec (or adding) portfolio to your services allows for better governance, and know how when things go wrong.
- All however must be Intertwined, and some points reviewed annually.
- Doing such allows for a large reduction in costs from reactive measures.

Risk Department Finds

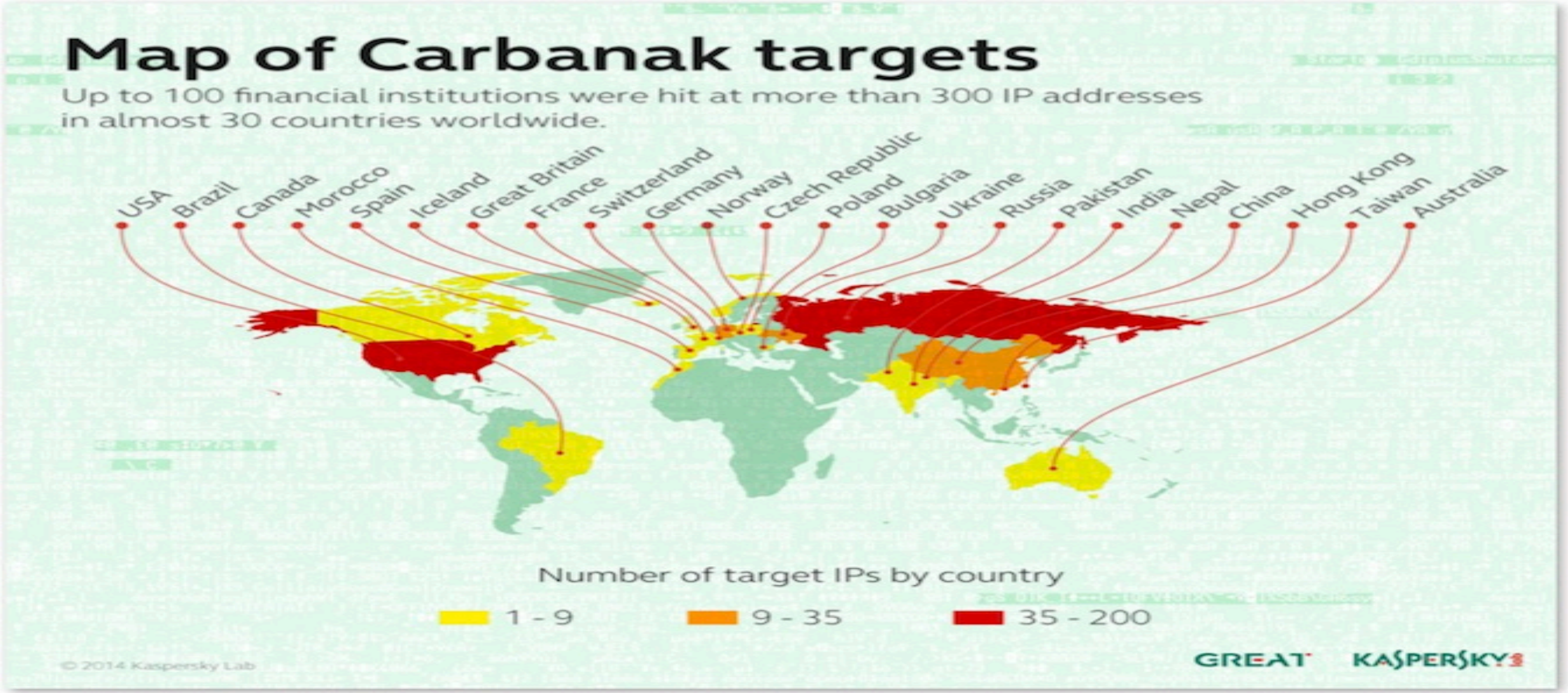
- Property Security Assessments – if the server room has no lock, your password will only work for so long
- TRAs – Threat Risk Assessments
- Investigations
- TSCM
- Other investigations
- Further security tools, services, - guarding, close protection, etc.
- Non InfoSec/Risk policy creation

Hacking Defined

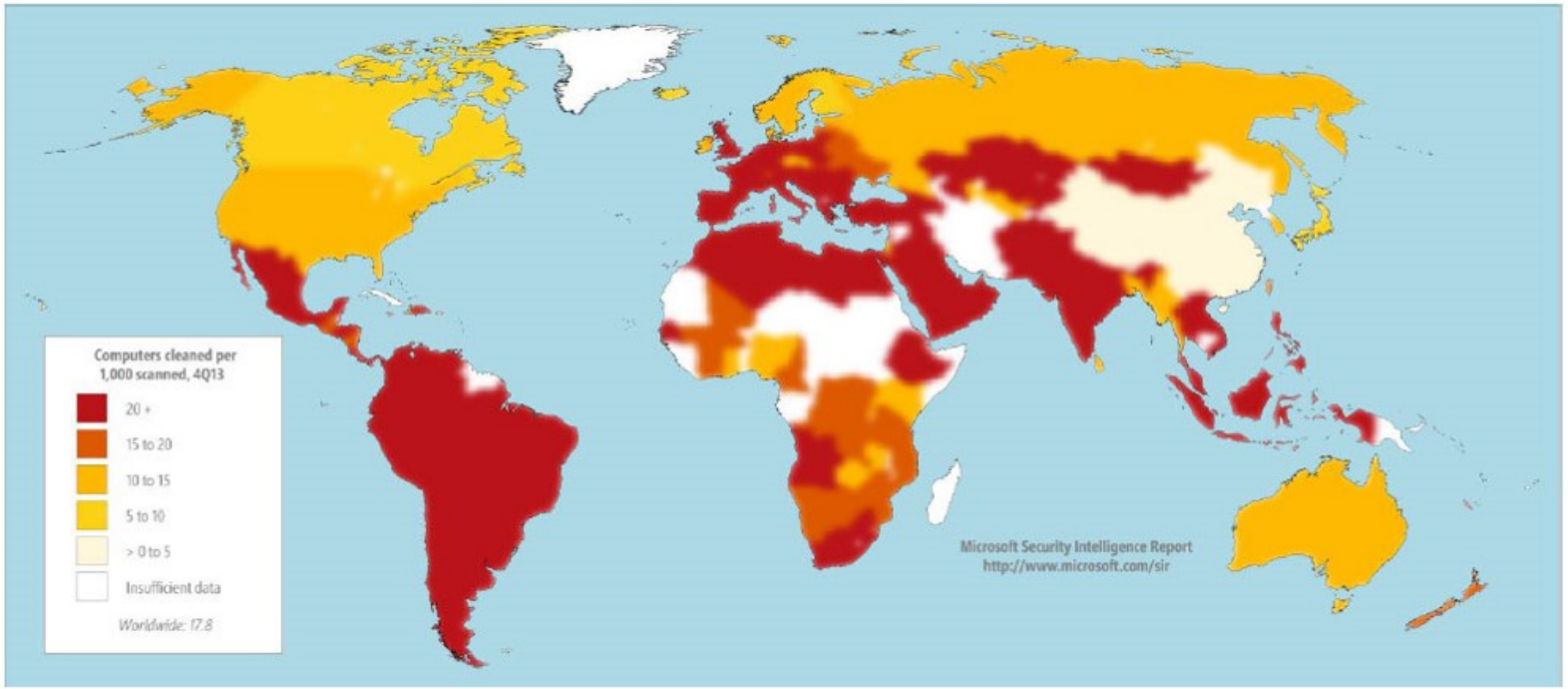
Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network.

Likelihood of being Hacked is??..... - Feb 15/2015

http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab



Interesting Report – end of 2013

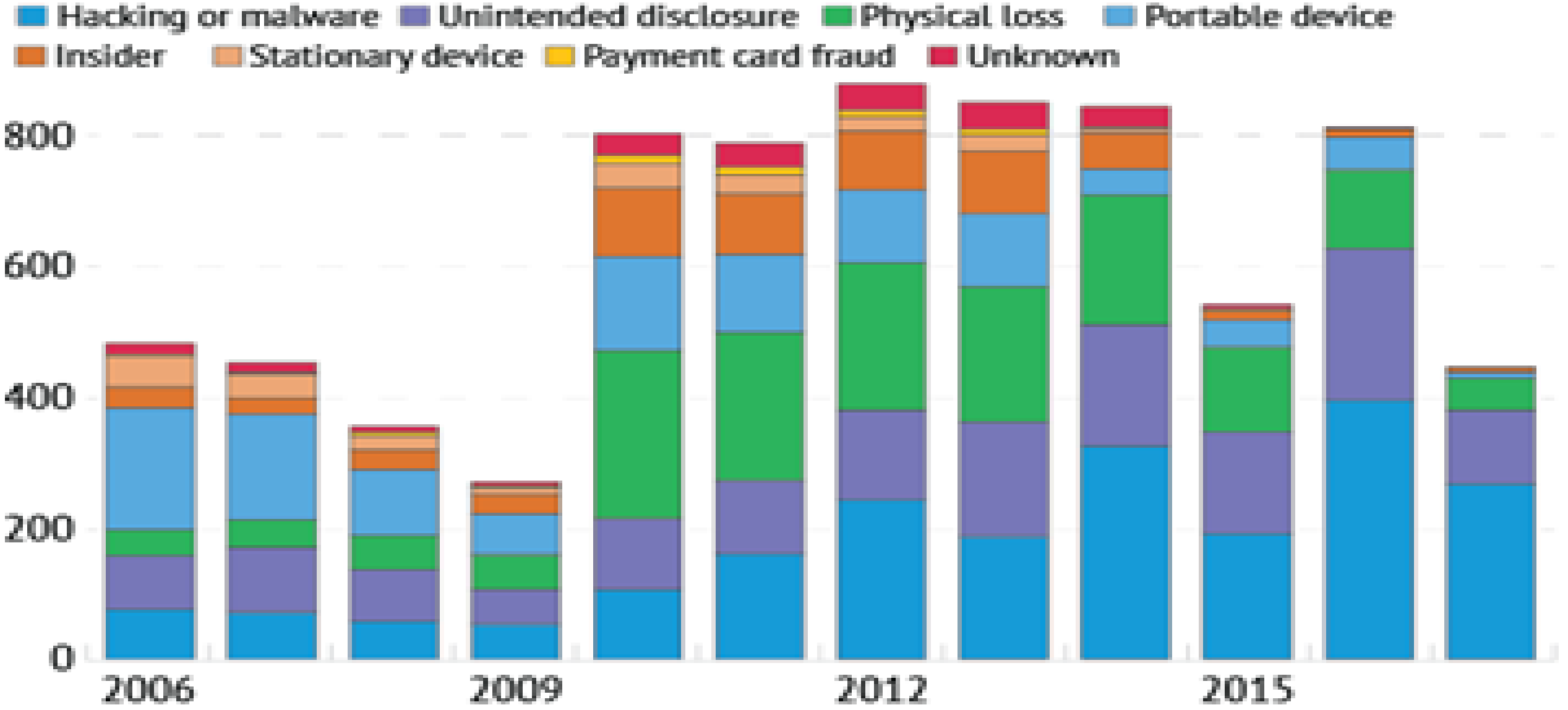


How to prevent it

- Best Practices
  - Standardize – know what is needed first and design the proper governance.
  - Build and test – penetration testing, should be more than just scanning IP numbers
  - Audit – maintain diligent and effective audit practices
  - Maintain the environment
- Resources
  - Make sure there is the right people to do the right job.
- Tools
  - Understand the tools you need
  - Maintain and integrate the necessary tools to protect the environment
  - Review what others are doing and trends
- Training
  - Maintain training yearly on the latest techniques and threats

Security incidents

Number of data breaches by type of breach, year of disclosure



Note: Date are through Oct. 2, 2017.
Source: Privacy Rights Clearinghouse

CNBC

What to Watch for

- Virus
- Trojans/worms
- Ransomware
- Hybrids
- Adware
- Spyware
- Fileless Malware

Every bank should know

Traces of Carbanak infection

Indirect attributes of Carbanak's presence in a bank network

A Paexec file

in Windows\ catalogue helping

to run commands on a remote machine

The billion-dollar advanced persistent threat is in your bank's network, if:

1. There are
files with .bin extension
at the following location:
\All users\%AppData%\Mozilla\
or c:\ProgramData\Mozilla\

2. There is
a svchost.exe file
in Windows\System32\com\ catalogue
(or Windows\Syswow64\com\ catalogue - for 64-bit OS Windows)

3. Among the active Windows services
the Services ending in "sys"
were found, duplicating a similar service
stored without the "sys"
Example: you find an instance of the aspnetsys service while the legal aspnet service is active on the system.

GREAT KASPERSKY

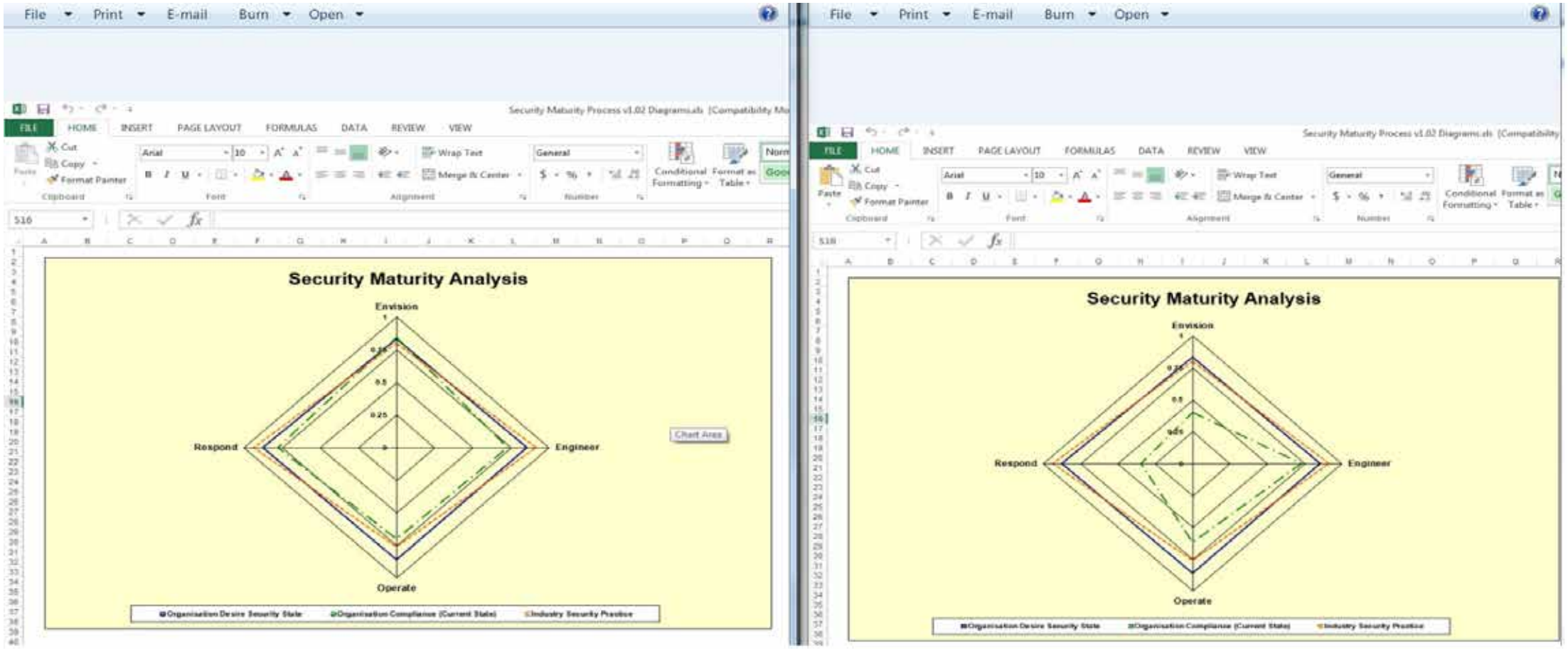
Develop your Risk Dept.

- Know where to get the talent – you don’t need staff for this
- Understand the pricing differences
- Follow a framework that works – ISO/Cobit, etc.
- Use the proper certifications – each means something different
- Understand the differences of the ‘computer guy/girl’.
- Medium small businesses need risk departments too, tailor
- Audit/ review yearly – more $$
- Stay current in trends, make sure who you use for risk tasks is too.

What can help balance your risk?

- SMA
- RISK ASSESSMENTS
- PRIVACY ASSESSMENTS
- SCHEDULES
- STANDARDS
- PROCEDURES
- REPORTS/REPORT REVIEWS
- CONSULTING RISK PROFESSIONALS

After and Before using SMA

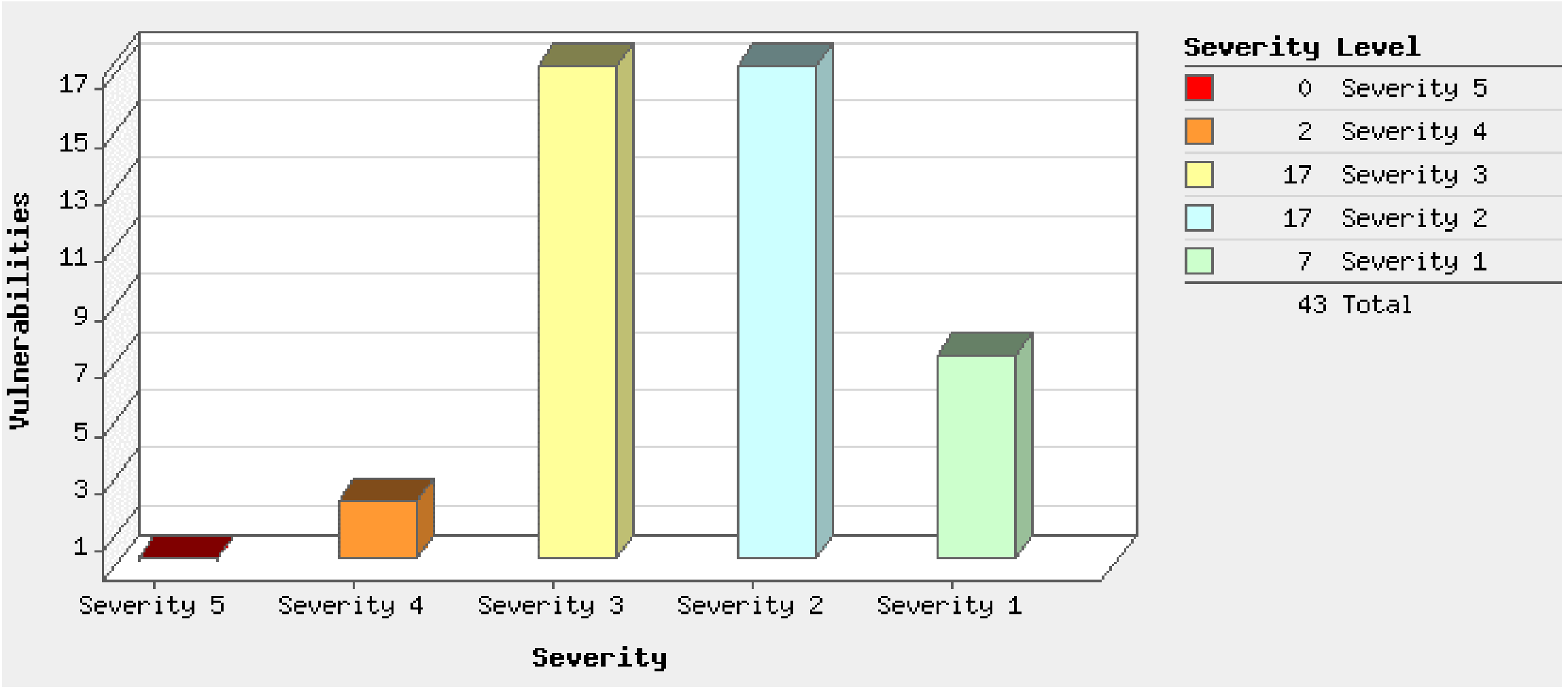


side by side comparison of states at Client using SMA.jpg

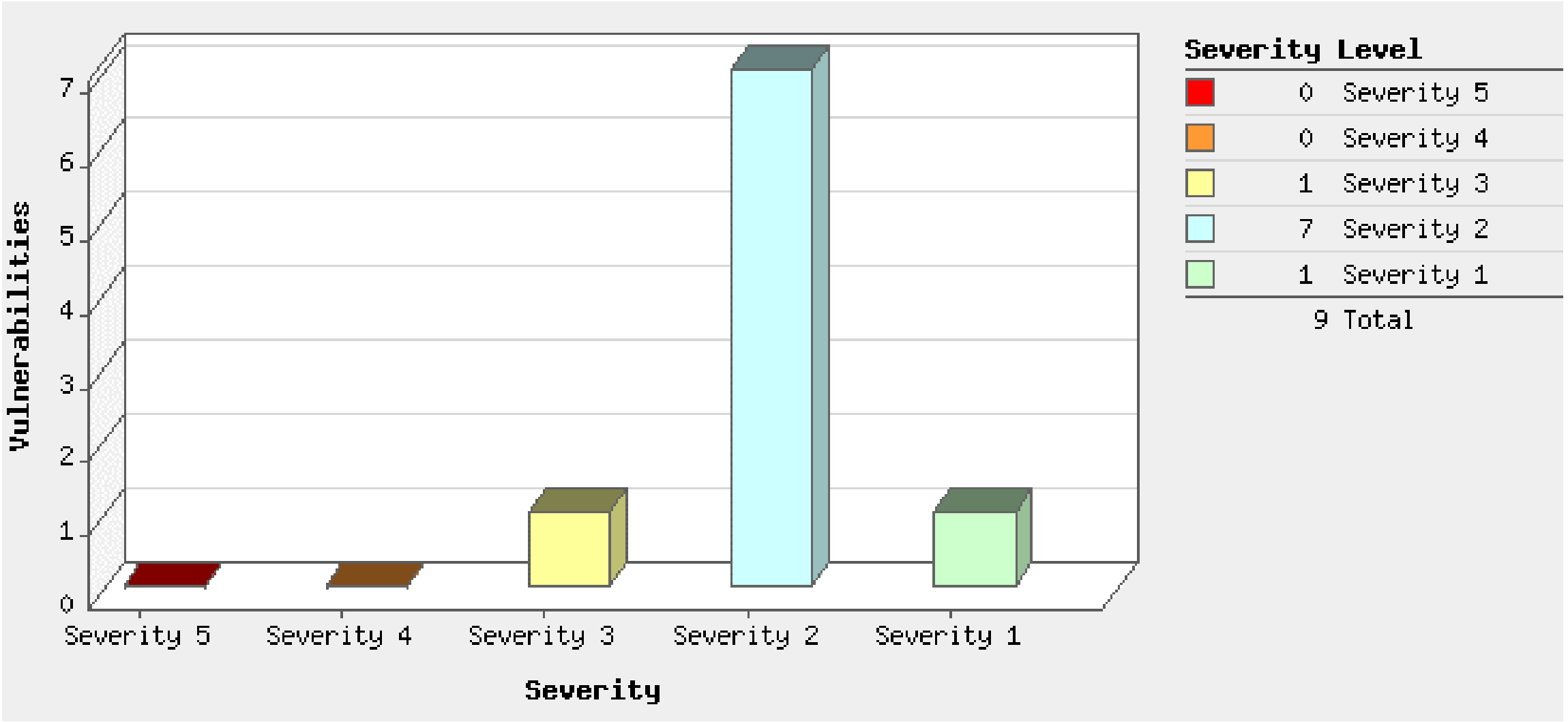
PNG image
firewall report fixed.png

Without Resource Attention

threat report fixed.png



With Resource



Maintain Secure Environment

What is needed?:

- Risk resource – discussion on FT, PT, Contractor
- Budget allocated for operations, tools
- Risk should include input from Executive Management, Board, Legal
- Risk duties, tasks, and portfolio should be outlined
- Risk and audit should NOT be the same department
- Audits of any kind by outsiders should be according to ISO framework. (best investment)
- Acceptance of the security strategy must be done by the Board and Executive Management.

What is Computer Forensics

- Computer forensics experts:
  - Identify sources of documentary or other digital evidence.
  - Preserve the evidence.
  - Analyze the evidence.
  - Present the findings.
- Computer forensics is done in a fashion that adheres to the standards of evidence that are admissible in a court of law. Thus, computer forensics must be techno-legal in nature rather than purely technical or purely legal.

What is found during a Forensic Review

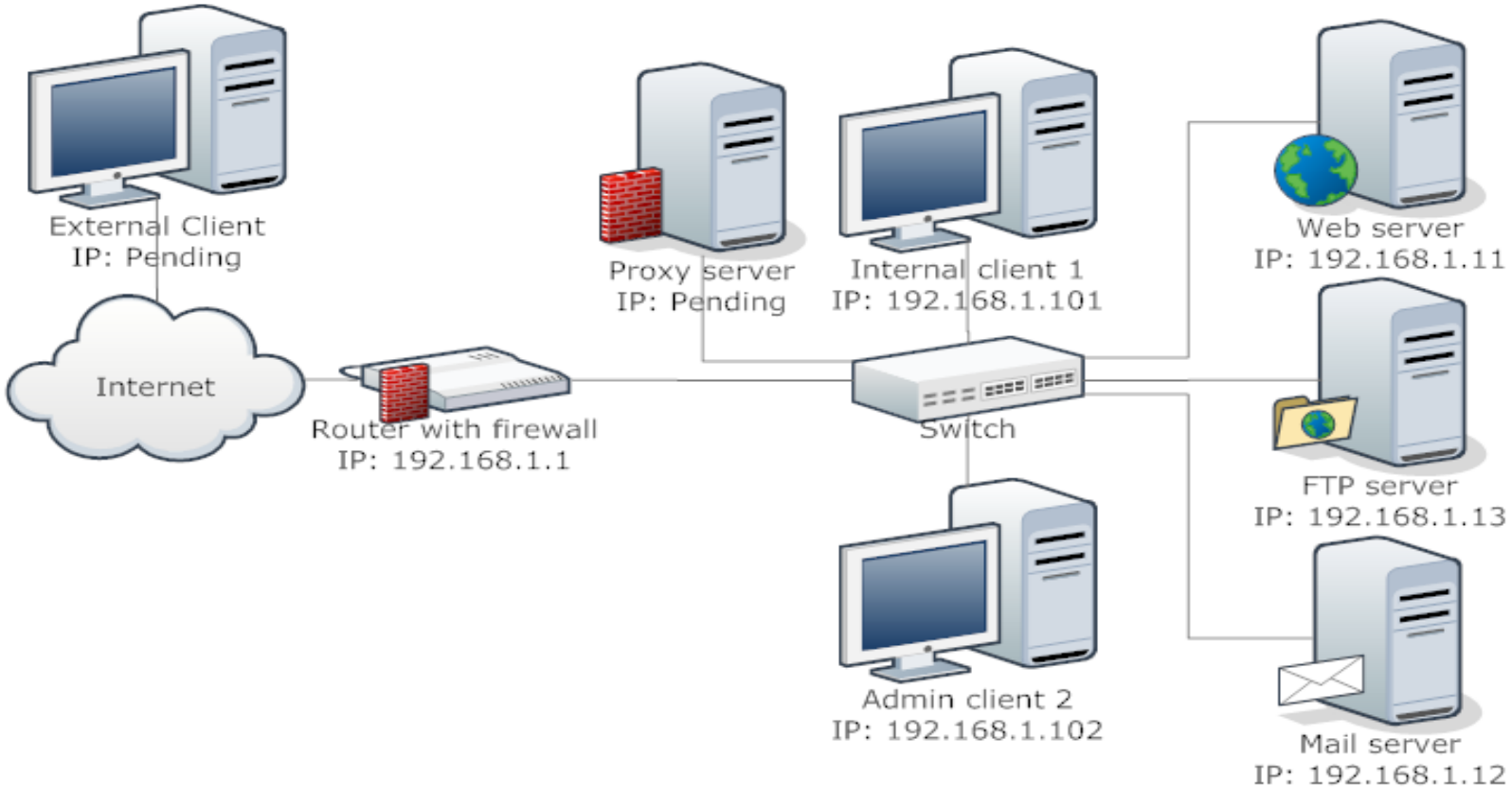
- Deleted, formatted or sometimes wiped information.
- Hidden or unseen files on a system.
- Information within certain files (pictures within a Word document – data carving)
- All web-based email account emails like Yahoo and Hotmail.
- History of what websites were viewed, what time, etc.
- All creation, modified, and accessed dates and times for almost all files and folders on the computer
- Times and dates when the computer was turned on and off, logged in and out.

When to perform a Forensic Review

- Upon knowledge of policy infractions
- Employee retirement or dismissal
- When Malware is found on a computer hard drive.
- If a system breach has occurred.
- If the computer was potentially used in a criminal act.

More than forensics – other locations.

- There are many locations to find evidence inside an organizations network.



Providing Awareness to your Staff

- Work with your Risk/InfoSec person to develop the right awareness program.
- Most awareness plans are fairly generic. A risk dept will know best how to tweak for the audience within an organization.
- Not best to ‘doom and gloom’.
- Find out if there have been issues in the past.
- Show them in material current stats, information, and how to make positive changes to safeguard the environment.
- As much as they think they are secure, they have likely not tested such.
- Review with them past audits, gaps & remediation plans.

ANY QUESTIONS?

www.net-patrol.com
twarren@net-patrol.com
905-334-2061